IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israel corporation, Plaintiff, v. SECURE COMPUTING CORPORATION, a Delaware corporation; CYBERGUARD CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100, Defendants.	)	C. A. No. 06-00369 GMS

DEFENDANT SECURE COMPUTING CORPORATION'S OPENING CLAIM CONSTRUCTION BRIEF

Fredrick L. Cottrell, III (#2555)
cottrell@rlf.com
Kelly E. Farnan (#4395)
farnan@rlf.com
Richards, Layton & Finger
One Rodney Square
P.O. Box 551
Wilmington, DE 19899
(302) 651-7700
Attorneys For Defendants

OF COUNSEL:

Ronald J. Schutz
Jake M. Holdreith
Christopher A. Seidl
Trevor J. Foster
Robins, Kaplan, Miller & Ciresi L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500

Dated: September 7, 2007

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

INTRODUCTION

Finjan's approach to claim construction ignores the canons of claim construction in favor of a transparently goal-oriented approach to defining terms. Finjan's approach is made clear by looking at the definitions Finjan proposed for Secure Computing's patents. Those constructions improperly read in several limitations from the preferred embodiment. For example, Finjan includes one or more limitations related to LDAP directories in every definition of every proposed construction of Secure Computing's '361 patent. With respect to Finjan's own patents, Finjan opted to use vague and ambiguous language to construe terms. The goal is simple, Finjan has included as many limitations as possible in Secure Computing's patents to leave a potential noninfringement argument. On the other hand, with respect to Finjan's own patents, Finjan provided ambiguous definitions that would allow Finjan to later mold the meaning of terms in order to avoid prior art problems and escape noninfringement arguments. This approach should be rejected in favor of Secure Computing's use of the proper rules of construction as outlined by the Federal Circuit.

I. LEGAL STANDARDS OF PATENT CLAIM CONSTRUCTION

Claim construction is the process by which this Court discerns the meaning of a party's claims, and thus what it owns. There are several key canons of claim constructions that are particularly significant to a proper construction of the claims in this litigation.

First, the words of a claim "are generally given their ordinary and customary meaning." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004). The

ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application. *See Phillips*, 415 F.3d at 1313.

This inquiry is an objective one, in which the court looks to those sources available to the public that show what a person of skill in the art would have understood disputed claim language to mean. *Id.* at 1314. Those sources include the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art. *Id.* This extrinsic evidence can include expert testimony on the background of the technology at issue, how a claimed invention works, and the knowledge and understanding of persons skilled in the art. *Id.* at 1318; *Pfizer, Inc. v. Teva Pharms. USA, Inc.*, 429 F.3d 1364, 1374 (Fed. Cir. 2005) (expert testimony supported conclusion on understanding of persons in the art). It can also include dictionaries and treatises. *See Phillips*, 415 F.3d at 1324.

Where a term has no ordinary meaning, the Court must look to the specification to see if a patent assigns a meaning. *Id.* at 1325.

Second, while the person of ordinary skill in the art is deemed to read the claim term in the context of the claims as well as the specification, *Ferguson Beauregard/Logic v. Mega Systems*, 350 F.3d 1327, 1338 (Fed. Cir. 2003), the Court must not at any time import limitations from the specification into the claims. *CollegeNet, Inc. v. ApplyYourself, Inc.*, 418 F.3d 1225, 1231 (Fed. Cir. 2005). As the Federal Circuit has explained,

> [C]laims are infringed, not specifications. . . . If everything in the specification were required to be read into the claims,

> or if structural claims were to be limited to devices operated precisely as a specification-described embodiment is operated, there would be no need for claims . . . It is the claims that measure the invention.

SRI Int'l, Inc. v. Matsushita Elec. Corp., 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc).

The foundation of this rule is the basic understanding that the law of patenting is intended to be reasonable. In other words, "[t]he law does not require the impossible. Hence, it does not require that an applicant describe in his specification every conceivable and possible future embodiment of his invention." *Id.* Thus, "[e]ven when the specification describes only a single embodiment, the claims of the patent will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope using 'words or expressions of manifest exclusion or restriction.'" *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 906 (Fed. Cir. 2004) (internal citations omitted).

These basic canons should guide this Court's construction of the disputed terms in Finjan and Secure Computing's patents. Secure Computing has set forth below each of the disputed terms, together with its proposed construction and the reasons supporting Secure Computing's construction. The parties have also separately filed a Joint Claim Chart that provides Secure Computing's constructions along with the intrinsic evidence that supports the phrases that Secure Computing believes should be construed.

II. THE '361 PATENT

A. Background of the '361 Invention

The invention disclosed in Secure Computing's '361 patent is a new and more efficient way for network administrators to set user and group-based security policies on

firewalls. Before the '361 patent, network administrators had begun maintaining information about users within a particular company on directory servers. These directory servers kept information related to users such as the user's name, the user's password, the user's position in the company (e.g. salesperson), and the user's phone number. These directory servers were a centralized way to maintain company information. '361 Patent, JA90 at col.2 ll.17-52.

The inventors of the '361 patent realized that these directory servers could used to set different permissions that different users on a network often have at the firewall to use certain resources. For instance, salespeople may have access to an internet-based application such as Salesforce.com, whereas engineers may not have such access. The directory servers contained centralized information about users and their positions that could facilitate setting specific permissions on a firewall without having to build and maintain separate lists for both the firewall and the directory server. '361 Patent, JA90 at col.2 ll.53-67.

The most popular directory servers at the time could be accessed through the use of a standard protocol known as Lightweight Directory Access Protocol (LDAP). Consequently, the inventors used a directory accessible by LDAP (LDAP directory) as an example of a directory server in the preferred embodiment. It is important to recognize, however, that "[e]ven when the specification describes only a single embodiment, the claims of the patent will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope using words or expressions of manifest exclusion or restriction." *Liebel-Flarsheim*, 358 F.3d at 906.

Using the invention disclosed in the '361 patent, network administrators are now able to maintain only one list of users and groups. Now, all of the firewalls within an organization can extract information from a network-accessible directory server in order to set user and group-based permissions. A network administrator need only build and update one list of users instead of manually updating multiple lists.

B. Construction of Claim Terms in the '361 Patent

In claim 1 of the '361 patent, a system grants a client access to a network resource. In practical terms, the system has (1) a server that has at least one directory; (2) the directory can be accessed using a network protocol and is configured to store information concerning an entity's organization; (3) a firewall that intercepts requests for network resources from client users on an internal network; (4) the firewall authorizes these requests for network resources based upon a comparison of contents in at least one entry in the directory to an authorization filter; (5) the authorization filter is based on directory schema that is predefined by the entity.

Secure Computing asserts that the plain language of the claims is clear and unambiguous to one of ordinary skill in the art and does not require construction. It is evident upon inspection of Finjan's proposed constructions that Finjan is not attempting to define terms but is merely using the exercise of claim construction to try to limit the claims to the preferred embodiment in an effort to avoid infringement.

1. "A server having at least one directory that can be accessed using a network protocol"

This phrase does not require construction. "A server having at least one directory that can be accessed using a network protocol" includes the terms, "server," "directory," and "network protocol" that were commonly understood to one of ordinary skill in the art

at the time of the invention. Furthermore, one of ordinary skill in the art understood that a server could have a directory that could be accessed using a network protocol, and therefore the phrase should be given its ordinary meaning within the context of the claim. It means a server that has at least one directory that can be accessed using a network protocol.

The specification of the patent illustrates that servers having directories accessible by a network protocol were known to those of skill in the art. As the specification states:

> A directory service includes all the functions of a directory and adds a network protocol that can be used to access the directory. Standardization is desirable in implementing a directory service.
>
> An early standard for directory service was the directory access protocol (DAP), which originated in the European standards organization. DAP although specifying a vast, feature-rich protocol for storing and encoding directory information, was unwieldy in size.

'361 Patent, JA90 at col.2 ll.28-37.

Finjan does not propose to define this phrase but only attempts to limit the plain meaning of these terms to the preferred embodiment disclosed in the specification. Finjan proposes that the phrase means "an internal server having an LDAP directory that stores information about users, offers a static view of information and allows simple updates without transactions."

Finjan does not dispute that the term "server" and "directory" are well known to one of ordinary skill in the art at the time of the invention since their own proffered constructions includes these same terms. Finjan has simply added modifiers and limitations from the preferred embodiment, ignoring the canons of claim construction. For example in the case of the term "server," Finjan repeats the word "server," but inserts the adjective "internal," a limitation that is not found in the claim language. The Federal

Circuit has specifically warned against inserting such limitations into the claims. *CollegeNet, Inc. v. ApplyYourself, Inc.*, 418 F.3d 1225, 1231 (Fed. Cir. 2005).

Finjan again does not attempt to define "directory." Finjan repeats the term "directory" and improperly adds that the claim is limited to an LDAP directory described in the preferred embodiment of the invention. Finjan's lack of a proffered definition of "directory" confirms Secure Computing's position that the term "directory" is understandable to one of ordinary skill in the art. Nowhere in the claim language does the claim require that the directory be an LDAP directory. The claim merely requires that the directory be accessible by some network protocol. It is true that an LDAP directory is an example of a directory that is accessible by a network protocol. No language in the claim necessitates that the directory service be the lightweight directory access network protocol directory.

Furthermore, Finjan ignores the doctrine of claim differentiation. For example, dependent claim 2 states that the "at least one directory is a lightweight directory access protocol directory." *See Liebel-Flarsheim.*, 358 F.3d at 910 (explaining that under the doctrine of claim differentiation, "the presence of a dependent claim that adds a particular limitation raises a presumption that the limitation in question is not found in the independent claim"). Even the examiner expressly noted that claims 2 and 9 further limit the claims from a general directory to an LDAP directory. '361 Prosecution History, Non-Final Rejection (mailed Sept. 10, 2003) JA2021 at 7. ("[C]laims 2 and 9 [] further limit claims 1 and 8 respectively by specifying the directory as being an LDAP directory.") If Finjan's proposed claim construction were to be adopted it would render these claims superfluous.

Finjan's position that "directory" means "LDAP directory" is further at odds with the applicant's statements made during prosecution. Applicant stated to the examiner that, "[a]pplicant teaches that it can be advantageous to configure the firewall to leverage existing database, **such as** an LDAP server storing employee information such as is shown in Fig. 4." Amendment and Response (received Jan. 20, 2004) JA2033 at 8, (emphasis added).

Finjan further rewrites the claims to add three more limitations to the term "directory." Finjan inserts language that requires the directory to (1) "store information about users," (2) "offer a static view of information" and (3) "allow simple updates without transactions." Again, Finjan ignores the plain language of the claim and inserts additional limitations from the background of the invention portion of the specification in an attempt to avoid infringement. *See* '361 Patent, JA51 at col.2 ll.17-24.

For these reasons, Finjan's construction of "a server having at least one directory that can be accessed using a network protocol" should be rejected.

2. "Authorization filter"

Secure Computing asserts that the term "authorization filter" should be given its plain and ordinary meaning in the context of the claims. All independent claims require that there be a comparison between the authorization filter and data obtained from the directory for authorization to occur. It is a filter that allows or disallows authorization, using information about the user as recited in other limitations in the claims.

The straightforward nature of the meaning of "authorization filter" is illustrated in the appeal brief filed by the applicant during prosecution. Here, the applicants explained: "[a]t its simplest, an authorization filter is an attribute and value pair. In the case of this example, the filter may be 'Department = Accounting' (i.e., the user must work for the

accounting department to be able to access the financial database server.)." *See* '361 Prosecution History Appellants' Brief on Appeal Under 37 C.F.R. 41.37(c), JA2177 at 12.

Finjan asserts that "authorization filter" means "a module to determine whether one or more attributes of the client user's LDAP entry is satisfied or whether the client user is a member of a group in the LDAP directory." (emphasis added) Finjan's proposed construction restates the function of the authorization filter that is recited in other parts of the claim, and attempts to add the limitation that the entries must be in an LDAP directory. This is just another occurrence of Finjan attempting to insert the preferred embodiment LDAP directory into the claims, and accordingly should be rejected by this Court. As already noted, dependent claims 2 and 9 add the limitation of an LDAP directory, and accordingly the limitation is presumed not to occur in the independent claims.

3. "Directory Schema that is predefined by said entity "

The claim language, "directory schema that is predefined by said entity" has a plain and ordinary meaning and does not require construction by the Court. It means what it says. Finjan again rewrites the claim language in an attempt to insert the preferred embodiment into the claims. Finjan asserts that a "directory schema that is predefined by said entity" means "an authentication scheme specified to interact with an existing LDAP directory that has been uniquely developed for an organization's internal needs" (emphasis added).

Nowhere in the independent claims does it state that the directory is an LDAP directory. For the third time, Finjan attempts to insert this limitation wherever it can. Furthermore, nowhere in the claim does it state that the directory has to be developed for

the organization's *internal* needs. As the claim states, the directory is merely predefined by the entity.

In addition, Finjan's rewriting of the claim language to define "directory schema" as "an authentication scheme" is misplaced. The point of the claimed invention as shown in undisputed limitations in the claims is to use a pre-existing directory and its entries for use by a firewall in authorizing certain requests made by users while also having the flexibility to use the directory for other purposes within the company. The directory schema does not have to be authentication specific. One object of the invention is to provide, for example, a "mechanism for leveraging an existing LDAP directory server as part of a firewall's authentication process." Therefore, "an existing LDAP directory can be used as a central directory that stores the data used by all applications." '361 Patent, JA90 at col.2 ll.62-67.

Finjan's construction is contrary to the plain language of the claims and unsupported by the record. Accordingly, it too should be rejected.

4. "Firewall"

Secure Computing submits that the term "firewall" is a common term of art and a person of skill in the art at the time of the invention would understand its meaning. Therefore "firewall" should be given its plain and ordinary meaning within the context of the claim.

The prosecution history of the '361 patent supports Secure Computing's position. In the Sept. 9 2003 non-final rejection, the examiner cited the Microsoft Computer Dictionary's 1997 definition of firewall, clearly illustrating that this is and was a common term of art at the time of the invention. *See* '361 Patent prosecution history, Sept. 9, 2003 office action, JA2018 at 4.

Finjan asserts that the ordinary meaning of "firewall" should be limited to a highly specialized "firewall that does not authenticate users using its own database but, rather, information contained within an LDAP directory." Again, it is clear that Finjan does not dispute that "firewall" is a common term since Finjan repeats the word "firewall" in its definition. Instead, Finjan attempts to rewrite the claim to insert language that unnecessarily limits the plain meaning of "firewall." Nowhere in the claims does it say that the firewall "does not authenticate users using its own database but, rather, information contained within an LDAP directory." This is a the fourth attempt by Finjan to insert the LDAP embodiment from the specification and therefore its proposed construction should be rejected.

Furthermore, Finjan's definition of the term firewall is unsupported by the specification. There is no indication that Secure Computing strayed from the common meaning of firewall in its specification. In fact, in the background of the invention section of the specification the patentees use nearly all of column 1 of the '361 patent to describe firewalls in the related art. The usage of the term "firewall" throughout the specification is consistent with the examiner's cited dictionary definition of firewall found in the prosecution history and therefore Finjan's construction should be rejected.

5. "Network protocol"

The term "network protocol" is a standard industry term and would have been understood to one of ordinary skill in the art at the time of the invention and therefore does not require construction.

Consistent with its overall strategy, Finjan does not provide a definition of the commonly understood term, "network protocol" but merely argues that the term is limited to one type of network protocol that is used in the preferred embodiment of the

invention, the "lightweight directory access protocol." Lightweight directory access protocol is the full name for the acronym LDAP. This is yet a fifth attempt by Finjan to read "LDAP" into the independent claims, in conflict with plain meaning and the doctrine of claim differentiation. For the reasons stated in the previous section regarding LDAP, Finjan's proposal should be rejected.

6. "Per-service authorization scheme"

First, the term "per-service authorization scheme" is referenced throughout the specification, but the claims use the phrase "per-service authentication scheme" (emphasis added). As Finjan has asked the Court to construe the phrase "per-service authorization scheme," in the joint claim construction statement it appears the parties agree that "per-service authentication" in the claims should be read as "per-service authorization.

The term "per-service authorization scheme" means what it says. It is an authorization scheme that grants access to a client user to a class of services. One example of a class of services is protocol services. This is clearly demonstrated in the specification.

> It should be noted that the authorization process need not be based on per-user authorization. In another embodiment, the authorization process can be based on a per-service authorization. In this embodiment, the per-service authorization can include an authorization for protocol services. Examples of protocol services include FTP, simple mail transport protocol (SMTP) e-mail, hypertext transport protocol (HTTP), etc. The per-service authorization can also be based on LDAP directory information. For example, authorization module 206 can use group memberships to determine whether a client user can use HTTP through firewall 210. To satisfy this authorization process, the authenticated user must be a member of the "web-users" group in the LDAP directory.

'361 Patent, JA92 at col.6 ll.32-45.

Finjan does not stray from its strategy of importing limitations from the specification when it proffers a construction for "per-service authorization scheme" as "a scheme in which the authorization module determines whether the user is in one or more groups in the LDAP directory in order to satisfy the authorization filter." The specification excerpted above makes clear that the authorization module's use of group memberships to determine whether a client user can use HTTP through the firewall is *an example*. "**For example,** the authorization module 206 can use group memberships to determine whether a client user can use HTTP through firewall 210." '361 Patent, JA92 at col.6 ll.41-43 (emphasis added)). Therefore Finjan's limitation of "group membership" should be rejected. Furthermore, Finjan again, for the sixth time, attempts to import the limitation of an LDAP directory into the claim and for the reasons stated above this should be rejected.

The term "per-service authorization scheme" should be given its plain and ordinary meaning in the context of the claim and Finjan's proposed definition should be rejected.

7. "Per-user authentication scheme"

The parties also appear to agree that the term "per-user authentication scheme" means "per-user authorization scheme" (emphasis added).[1] Like the term "per-service authorization scheme," this term also has a plain and ordinary meaning and does not require construction. It is an authorization scheme that allows access on a user-by-user basis. The specification makes this clear. In presenting the example of a preferred embodiment:

[1] In particular, Finjan's definition refers only to an authorization module as opposed to an authentication module. *See* Joint Claim Chart, Docket No. 108.

> If per-user authorization is configured, authorization module 206 determines whether one or more attributes of the client user's LDAP entry satisfies an authorization filter. If the one or more attributes of the client user's LDAP entry does not satisfy the authorization filter, then authorization module 206 determines that the authorization fails. If the authorization filter is satisfied, then the client user's network resource request is allowed through firewall 210. This allowed connection is illustrated in FIG. 3 as path 310.

'361 Patent, JA92 col.5 ll.25-33.

Finjan purports that a "per-user authorization scheme" is "a scheme in which the authorization module determines whether one or more attributes of the client user's LDAP entry satisfies the authorization filter" (emphasis added) Again, for the seventh time, Finjan repeats the language of the claim, but attempts to limit the plain and ordinary meaning of a claim term to include the limitation to a specific directory, namely an LDAP directory. For the reasons stated above, this should be rejected and Secure Computing's construction should be adopted.

III. THE '010 PATENT

A. Background of the '010 Invention

The inventors of the '010 patent conceived of a novel way to allow people from outside a company to request internal documents without risking the disclosure of proprietary information. Prior to the invention, people who wished to access internal documents from outside a company were either given access to the entire internal network or they were given access only to an external web server. '010 Patent, JA72 at col.1 ll.43-59. The inventors came up with a way to allow outsiders selective access to files on the internal network. In particular, the inventors described a document server that evaluates requests for internal files and authorizers particular users to access those documents based on the group to which they belong. *Id.* at col.2 ll.1-10. For instance, re-

sellers are able to access certain internal documents over the web while salespeople are able to access different internal documents over the web.

B. Construction of Claim Terms in the '010 Patent

1. "Document control server"

The phrase "document control server" means what it says and should be given its plain and ordinary meaning within the context of the claims. It means a server that controls a user's access to documents on a document server. The plain and ordinary meaning of this term is clearly set forth in the context of the claims. For example, claim 11 recites, "wherein the document control server receives a document request from the external interface for the first document, determines a user associated with the document request and authenticates the user; and wherein the document control server includes a go list processor for determining, based on the document list, if the user has authorization to access said first document." '010 Patent, JA80 at col.17 ll.42-50.

The specification also makes clear that the "document control server" determines which users can access documents on the document server. "The document control server includes a go list processor for determining if the user has authorization to access said first document and a document processor for reading the first document from the document server..." '010 Patent, JA72 at col.2 ll.18-21.

Finjan proffers a definition that is pulled straight from a preferred embodiment of the invention. Finjan argues that "document control server" means "a mechanism which allows a specified business partner to access documents on another company's non-public internal network." Nowhere in the claims does it require that the server allows access to "specified business partners." It is clear from the context in claim 11 and the specification at col.2, l.19 that the document control server controls access to simply a

"user" not a "specified business partner." Furthermore, the claims require that the document control server authorize access to documents on a document server only. *See, e.g.*, '010 Patent, JA80 at claim 11. Nowhere in the independent claims does it require that the documents that are accessed be located on "another company's non-public internal network."

2. "Fetching the requested document"

The phrase "fetching the requested document" has an ordinary meaning to one of skill in the art at the time of the invention and does not require construction. The phrase means, "fetching the requested document" and is the same as retrieving or reading the requested document. For example, the specification gives multiple examples in which a requested document is "retrieved."

> "If so, at 36, **system 10 retrieves the document from document server** 14, cleans the document at 38 and, at 40, forwards the clean version of the document to the user." ('010 Patent, JA73 at col.3 ll.40-42, emphasis added.)
>
> "**Document processor 24 reads a document from document server** 14, cleans the document as detailed above and forwards a clean version of the document to the user." ('010 Patent, JA75 at col.7 ll.49-53, emphasis added.)

One can easily recognize that the inventors were using the word "retrieve" synonymously with "fetch" because the order of operations consists of (1) retrieving, (2) cleaning; and (3) forwarding. When one looks to the specification for examples of the word "fetch," the same pattern is described. For example, the summary of the invention states that "the requested document is fetched, cleaned and sent to the client." '010 Patent, JA72 at col.2 ll.9-10.

Finjan argues that the simple task of "fetching the requested document" includes "obtaining, parsing and cleaning the document." This is clearly erroneous when viewed

in light of the specification. The excerpts from the '010 patent shown in the above paragraph illustrate that the act of "fetching" is separate and apart from the actions of, for example, "cleaning" and should not be read into the claims as Finjan argues.

In fact, Finjan's proposed construction reads out a preferred embodiment of the invention: the embodiment where the document control system retrieves non-text documents. In this embodiment no "parsing" is done to the document. "The pages returned by the intranet are categorized as either text or non-text. Examples of the latter are graphics, such as GIF or JPEG documents, sound objects, or executable objects, such as Java applets. **Non-text pages are not parsed and forwarded back to the client browser unchanged.**" '010 Patent, JA74 at col.5 ll.7-12 (emphasis added). Therefore, if the Court were to adopt Finjan's proposed construction in which "fetching" means "obtaining, parsing and cleaning" this would preclude the claims from reading on the embodiment in the specification wherein the system retrieves non-text documents such as GIF, JPEG documents, sound objects or Java applets. This violates the canons of claim construction and Finjan's construction should be discarded. *See, e.g.*, *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 865 (Fed. Cir. 2004) ("[A] construction that excludes a preferred embodiment 'is rarely, if ever, correct.'").

3. "Proxy"

The term "proxy" is a well known term of art and does not require construction. The claims, specification, and file history support its plain and ordinary meaning. For example, the specification outlines the use of a proxy in a preferred embodiment stating that the proxy functions to hide the address of the document sought.

> 1) Redirected proxy--For added security on external to internal connections, a redirected proxy can be configured on your firewall to redirect the inbound connection requests. When a Business Partner on the external network attempts to

> connect to document control server 12, firewall 40 intercepts the request and establishes a connection to server 12. **This rerouted connection hides the actual destination from the Business Partner requesting the connection.**
>
> 2) Transparent proxy--A transparent proxy can be set up through firewall 40 to document control server 12. **From the Business Partners' perspective it will appear as though they are connecting directly to server 12 and not connecting to the firewall first.**"

'010 Patent, JA78 at col.13 ll.55-67 (emphasis added).

This is consistent with the applicant's characterization of a proxy during prosecution of the '010 patent. When overcoming the Kitain reference the applicant stated that there was "no discussion in Kitain of the use of a proxy function to hide the address of the document sought." '010 Patent prosecution history, July 27, 2001 Amendment and Response, JA2041.

Finjan's proposed construction for "proxy" is "a process performed by a firewall in which the actual destination on the internal network is hidden from the business partner who is requesting the connection from an external network" (emphasis added). Secure Computing does not disagree with Finjan that a proxy acts to hide the destination of a file from a requesting client since this is the basic and ordinary meaning of the term. Secure Computing disagrees that elements from the preferred embodiment should be inserted into the ordinary meaning of "proxy." For example, in claim 1 a client has made a request for a document and the document is fetched as a proxy and sent to the client. *See* '010 Patent, JA79 at col.16, l.39 ("...associating the request with a client..."); "...fetching the requested document as a proxy and sending the requested document to the client." *Id.* at col.16 ll.43-44. There is no language that would limit this to a "business partner who is requesting the connection from an external network." The claim merely states that it is a client making the request.

Furthermore, Finjan continues to rewrite the claim by limiting the term "proxy" to hiding destinations on the "internal network" from business partners on the "external network." The only limitation in claim 1, for example, regarding internal versus external networks involves where the document is actually stored. The claim requires *only* that the document be stored on the internal network. '010 Patent, JA79 at col.16, ll.36-37. There is no limitation in the claim specifying from where the client request must originate.

For the reasons stated above Finjan's construction of "proxy" should be rejected.

4. "Role"

The term "role" as used in the specification and claims means "membership in a group of one or more." The term role is used in more than one way in the specification, so it is necessary to define the term in the context of the claim language. The claim language refers to the assignment of "clients" to a role and "users" to a role. *See, e.g.*, '010 Patent, claim 1 and 37. Based on this context the term "role" takes its plain meaning of a "membership in a group of one or more."

Finjan submits that "role" means "an alias which provides access to a list of allowed documents." The term "alias" as used in the specification is used to describe a directory path assigned to a specific server. However, this use of "role" in the specification is clearly set forth as one of the embodiments of the invention and therefore the term "role" should not be so limited. The specification states,

> To further reduce any bottleneck, **in one embodiment** document control server 12 includes the option for the actual "data owners" themselves to define which partners have access to selective internal data. A data owner is a trusted individual within the organization that is empowered to grant Business Partners access privileges to Web pages on document servers 16. **In one such embodiment, a Data Owner is assigned to one or more "roles," where a "role" represents the mapping alias assigned to one or [sic (of)] the servers** 16. A Data

> Owner can only add Business Partners or map URLs for the server "role" to which the Data Owner is assigned.
>
> For example, an employee working in the Accounting department would be assigned to an Accounting role (server)."

'010 Patent, JA74 at col.6 ll.43-57 (emphasis added).

Finjan ignores an alternative embodiment described in the specification wherein one server can contain information relevant to many roles. As the specification states:

> In one embodiment each user has one or more roles associated with their user ID. For instance, they could be in the Marketing role, as well as the Engineering role. In one such embodiment, each role is directly associated with an internal server; you can only define one role for each server. This means you could not have the Marketing role and the Engineering role going to the same physical internal server. Such an approach can simplify system design.
>
> In another embodiment, more than one roles may be assigned to each internal server. For example, a manufacturer may have all his reseller information on one server. One role, however, contains international resellers and another role contains domestic resellers. In such an embodiment, it would be advantageous to be able to define different sets of URLs on a single document server 14 that would allow for the different roles.

'010 Patent, JA73 at col.4 ll.27-34.

Finjan's proffered construction falls in line with the first embodiment described above wherein "you can only define one role for each server." However, Finjan's proffered definition erroneously reads out the alternative embodiment wherein "more than one roles may be assigned to each internal server" set forth in the second embodiment described above. *See, e.g.*, *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 865 (Fed. Cir. 2004) ("[A] construction that excludes a preferred embodiment 'is rarely, if ever, correct.'"). This is clearly indicative of Finjan's flawed logic. There is no language in the claim that precludes having more than one role assigned to each server

and therefore Finjan's construction should be discarded and Secure Computing's definition adopted.

IV. THE '194 PATENT

With respect to Finjan's asserted patents, Secure Computing shows that certain terms have no ordinary meaning and must therefore be defined. Secure Computing further shows that several terms in Finjan's patents are indefinite under 35 U.S.C. § 112.

A. Construction of Claim Terms in the '194 Patent

1. "Addressed to a Client"

The term "addressed to a client" is a broad phrase that could have more than one meaning to one of ordinary skill outside the context of the specification. For example, if a client meant either a computer or a person making a request, then the meaning of addressed to a client may be entirely different then its proper construction. However, the applicant made clear his intention to narrowly define "client" as the destination computer thus disclaiming any other meaning. Consequently, the term "addressed to a client" means that the "Downloadable" must contain the destination computer's Internet Protocol (IP) address. The specification makes clear that the phrase "addressed to a client" is referring to the IP address included in data packets sent to the client computer. A brief technical background is helpful before examining the support for this construction.

a. Technical Background

Most of the information communicated over local area networks (LANs) and the Internet is transferred using a standardized method or protocol known as TCP/IP. The TCP/IP protocol allows data to be split up into small packets that are sent separately over the internet between one or more computers. To allow each packet to find its destination, each computer or device on a network is assigned a unique number known as an IP

address. An IP address is roughly equivalent to a phone number or street address for the computer. In short, IP addresses allow one computer to uniquely address a packet of data to another computer. For example, Secure Computing's website is publicly accessible from a web server with the following IP address: 66.45.10.76.

A computer requesting information is typically referred to as the "client" and a computer that responds to the request is typically referred to as the "server." The server splits its response, for example a webpage, into small data packets that the server addresses to the client computer using the client computer's IP address in each packet. The client computer's IP address is recorded in each packet as the destination address. The data packets are then routed to the client computer using the destination IP address listed in each packet.

b. "Client"

In order to define the phrase "addressed to a client," it is first necessary to define the term "client." The '194 patent makes clear that the "client" is the computer requesting information. For instance, claim one contains the limitation of "preventing the execution of the Downloadable by the client." *See, e.g.*, JA17 at col.10 ll.16-17. Because the client is capable of executing the Downloadable, the claim must be referring to a computer. The applicant made this distinction even more explicit by incorporating U.S. Patent Application No. 08/790,097, which became U.S. Patent No. 6,167,520 ("'520 Patent"), by reference. In the '520 application, the applicant stated that a client is "e.g., an individual computer, a network computer, a kiosk workstation, etc." '520 Patent, JA2008 at col.2 ll.57-59; *see also* '520 Patent, JA2003 fig.2, JA2009 at col 3 ll.1-41 (explaining the hardware potentially included on client computers).

Accordingly, "client" is the computer from which the user is making a request.

c. "Addressed"

Because the specification makes clear that the "client" to which a Downloadable is addressed is a computer, one of ordinary skill in the art would understand that the term "addressed" means containing the client computer's IP address. In particular, one of ordinary skill would understand that the verb "addressed" would mean referring to the address of a device. For example, the IBM Dictionary of Computing gives the verb "address" the following definition: "to refer to a device or an item of data by its address." JA2071, George McDaniel, IBM Dictionary of Computing 13 (1994). Recognizing that the '194 patent is related to "a system or method for protecting a computer and a network," one of ordinary skill would identify the IP address as the unique address used to identify computers in network communications.[2]

Consequently, the phrase "addressed to a client" means "containing the IP address of the client computer."

d. Finjan has admitted that Secure Computing's Construction is Correct

In international prosecution of the same patent application, Finjan admitted that addressing information to clients, as discussed throughout the specification, means addressing data packages to particular client computers. Int'l Pub. No. WO 98/21683 (filed Nov. 6, 1997). The international application was filed on the same date as the '194

[2] *See, e.g.*, JA2072, McDaniel, at 354 ("**Internet address** The numbering system used in TCP/IP Internetwork communications to specify a particular network or a particular host on that network with which to communicate."); JA2076, Barron's Dictionary of Computer and Internet Terms 195 (5th ed. 1996) ("**IP Address** the numeric address of a machine, in the format used on the Internet."); JA2079, Dictionary of Computer Words 144 (1995) ("The unique numerical sequence that serves as an identifier for an Internet server.")

application and included the exact same specification. During prosecution, the applicants admitted:

> [I]t would have been routine knowledge for the man in the art that the operation of the Internet and of computer networks involves the addressing of data, e.g. in the in the form of data packages, to individual computers and that the references in the present application as originally filed to Downloadables being addressed to particular clients necessarily involved such Downloadables being incorporated in data or data packages addressed to particular client computers . . . .

JA2064, Int'l Pub. No. WO 98/21683, Reply to Examination Report (dated Dec. 21, 2005) (emphasis added). As noted above, a data packet is "addressed to particular client computers" by including the client's IP address in the packet. *See* Footnote 2.

This admission proves that one of ordinary skill in the art would understand that "addressed to a client" means "containing the client computer's IP address."

2. "Downloadable"

To one of skill in the art, the term "Downloadable" has no ordinary meaning. Stecher Depo. JA2158 at 74:20-24. Both parties accordingly agree that the term "Downloadable" requires definition. When a term has no ordinary meaning, the patent specification is the best source to determine its meaning. *Phillips*, 415 F.3d at 1315.

Both parties agree that a downloadable takes the form of "a program or document containing" something. There is disagreement between the parties over the particular information that the program or document must contain.

Secure Computing proposes that a "Downloadable" in the '194 patent's claims is "a program or document containing an executable application program that can be downloaded from one computer to another computer." The proof is quite straightforward. The first column of the patent specification expressly states: "A Downloadable is an

executable application program, which is downloaded from a source computer and run on the destination computer." '194 Patent, JA13 at col.1 ll.44-47.

Finjan proposes that the definition of "Downloadable" is "a program or document containing mobile code." The term "mobile code," however, does not appear anywhere in the specification. Finjan's proposed construction, therefore, is at odds with the Federal Circuit's requirement that one must look to the specification first when defining terms without an ordinary or customary meaning.

The one and only time that the applicant referred to "mobile code" was in a response in the prosecution history dated October 27, 1999. '194 Patent prosecution history, Preliminary Amendment (dated Oct. 27, 1999) at JA2051. It is neither necessary nor appropriate to overlook the clear definition in the specification in favor of an unclear statement in the file history. Indeed, the applicant does not even define what "mobile code" is. This Court, therefore, would need to construe the phrase "mobile code." That would be unnecessary and improper. *See, e.g.*, *Epicrealm, Licensing, LLC, v. Autoflex Leasing, Inc.*, Nos. 2:05CV163, 2006 WL 3099603, at *5 (E.D. Tex. Oct. 30, 2006) (JA2083-84) (disapproving of construction that would necessitate further claim construction); *Collegenet, Inc. v. XAP Corp.*, No. CV-03-1229-HU, 2004 WL 2429843, at *20-21 (D. Org. Oct. 29, 2004) (JA2111-12) (rejecting defendant's proposed definition, which added new, undefined phrases); *Pipe Liners, Inc. v. Pipeling Prods, Inc.*, No. Civ. A. 98-164 (SLR), 1999 WL 1011974, at *5 n.3 (D. Del. Oct. 22, 1999) (JA2136) (dismissing plaintiff's expert's proposed definition because, *inter alia*, it rests on an undefined term).

Secure Computing's proposed definition, which comes from the '194 patent's specification, therefore, should be accepted.

3. Server that Serves as a Gateway to the Client

The phrase "server that serves as a gateway to the client" means "a computer that receives data from its external communications interface and transfers the data through its internal communications interface to the client." The phrase "server that serves as a gateway to the client" does not have an ordinary meaning to one of skill in the art. "Gateway" is a marketing term that does not have a clear technical meaning. Gallagher Depo., JA2155 at 188:4-20.

As shown previously, when a phrase has no ordinary meaning, the specification provides the best guidance as to the meaning of the phrase. In this case, the specification does not use either the term "gateway" or "server." It is therefore necessary to infer from the claims that the "server that serves as a gateway to the client" is a structure that receives an incoming Downloadable. *See, e.g.*, '194 Patent, JA17 claim 1 ("[R]eceiving an incoming Downloadable addressed to a client, by a server that serves as a gateway to the client.").

The specification identifies the internal network security system as the structure that performs the step of "receiving an incoming Downloadable" by receiving the Downloadable through its external communications interface as illustrated in Figure 2. *See* '194 Patent, JA14 at col.3 ll.27-35; *id.*, JA4 at fig.2. Consequently, the internal network security system depicted in Figure 2 is the only structure that could be the "server that serves as a gateway to the client."

Figure 2 demonstrates that the internal network security system must use an "external communications interface" to receive an incoming Downloadable from an

external network. The external communications interface is illustrated at reference number 210 in the drawing. The "server that serves as a gateway" as illustrated in Figure 2 must also use an internal communications interface to forward the information to the internal network. '194 Patent, JA14 at col.3 ll.27-35; *see also* JA 4 at fig.2 ref. num. 225. The specification provides one other alternative: the external communications interface and internal communications interface can be functional components instead of separate devices. *Id.* JA 14 at col.3 ll.35-41. In both cases, the server that serves as a gateway to the client receives data directly from the external network through an external communications interface and transfers that data directly to an internal network through its internal communications interface. Consequently, the phrase "server that serves as a gateway to the client" means "a computer that receives data from its external communications interface and transfers the data through its internal communications interface to the client."

4. Claims 8, 9, 10, and 11 Are Indefinite Because They Claim Unfixed and Indefinite Trademarks.

Claims 8 through 11 in the '194 patent improperly include trademarked products as limitations. Claims 8 through 11 claim the following trademarks as limitations: Java™, ActiveX™, JavaScript™, and Visual Basic™[3] ("the trademarked products"). '194 Patent, JA17 at col.10 ll.34-41. The PTO's guidelines are clear, however, that a claim is indefinite if a trademark serves as a claim limitation. "If the trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the

[3] Claims 8 through 10 include a "™" symbol following each trademarked term. Claim 11, however, does not include such a symbol following Visual Basic. Visual Basic, nonetheless, is a registered trademark of Microsoft Corporation. *See* Trademark Registration Number 1787376. JA2163-64.

claim does not comply with the requirements of the 35 U.S.C. 112, second paragraph." Manual of Patent Examining Procedure (MPEP) § 2173.05(u) (2006). The Patent and Trademark Office Board of Appeals' likewise has ruled in *Ex parte Simpson* that trademarks are indefinite claim limitations. 218 USPQ 1020 (Bd. App. 1982). Claims 8 through 11, consequently, are indefinite.

In *Simpson*, the applicant included a trademarked product – Hypalon (a type of synthetic resin) – in his claims. *Id.* at 1021-22. Even though those skilled in the art knew that Hypalon was associated with an elastometric chlorosulphonated polythene and how to make such materials, the Board of Appeals nonetheless upheld the examiner's finding that the claims that included Hypalon were indefinite. *Id.* at 1021-22. The Board of Appeals explained that nothing in the record indicated "that materials marketed under the trademark 'Hypalon' contain only chlorosulphonated polythene." *Id.* at 1022. The applicant's use of the trademark, moreover, failed to provide definitive terminology of what the public was not free to use. *Id.* The applicant, for instance, failed to explain how much, if any, chlorosulphonated polythene must be present before infringement occurs. *Id.* The Board of Appeals, therefore, upheld the examiner's denial of all claims that included Hypalon. *Id.*

Simpson holds that trademarked products used as limitations in claims – even if known to those skilled in the art – do not adequately define the contours of the claims. Claims that include trademarked products as limitations fail § 112, paragraph 2's definiteness requirement.

Claims 8 through 11 do not meet § 112, paragraph 2's requirements as explained in the MPEP and *Simpson*. On the face of the claims, the trademarks are used

as limitations that identify particular products. All of the trademarked products in the '194 patent are simply brand names that identify specific products. The use of the trademarked products in the '194 Patent raise particular concern because none of them have fixed meanings. *See, e.g.*, David Chappell, Introducing ActiveX, JA2159 ("It's just not possible to give a clear technical definition of what the term ActiveX means. The reason for this is simple: ActiveX is a marketing label, not a technical term."). The public, therefore, is at the same peril as in *Simpson*. Just as the public in *Simpson* would not know how much chlorosulphonated polythene constituted Hypalon, 218 USPQ at 1022, the public similarly does not know when something meets the untechnical definition of the trademarked products claimed in the '194 patent. Claims 8 through 11 are, therefore, indefinite.

V. THE '780 PATENT

A. Construction of Claim Terms in the '780 Patent

1. "Performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID"

Secure Computing proposes that the phrase "performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID" should be construed as "performing a hashing function on both the Downloadable and the fetched software components together to generate a single Downloadable ID." This is because the plain language of the claim dictates the construction, and the applicant clearly surrendered any other construction during prosecution. *Southwall Techs., Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1576 (Fed. Cir. 1995) (holding that an applicant surrenders claim scope during prosecution by words of manifest restriction). The core of the proposed construction is the recognition that the Downloadable ID is generated from

both the Downloadable ***and*** the fetched software components. The claim language, the specification, and the prosecution history all support this proposed construction.

First, the claim language itself indicates that Secure Computing's construction is correct. The claim is written in the conjunctive. ('780 Patent, JA37 at col.10 ll.30-32.) Both the Downloadable and the fetched software components are necessary to generate a Downloadable ID. *See* '780 Patent, JA37 claim 1 ("[P]erforming a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.") (emphasis added). The claim thus cannot be read to generate a Downloadable ID based on the Downloadable alone or the fetched software components alone. Intrinsic evidence further confirms Secure Computing's proposed construction.

The specification, for instance, explains that the Downloadable ID is generated through a hashing process including both a Downloadable and some or all fetched components. '780 Patent, JA37 at col.9 ll.58-67. Figure 8 in the '780 patent, moreover, shows the method for generating a Downloadable ID. The figure illustrates that the ID generator receives both a Downloadable and fetched components before it performs the hashing function. '780 Patent, JA32 Fig.8. Once the hashing function is performed, the Downloadable ID is generated. The specification, thus, is consistent with the claim. Both require a Downloadable and fetched components to generate a Downloadable ID.

The prosecution history is similarly unambiguous and particularly telling. "Specifically, the **present invention** fetches software components required by the Downloadable, and performs a hashing function on the Downloadable **together with** its fetched components." '780 Application, Amendment and Response to Office Action (dated July 31, 2003) at JA2060 (emphasis added). The Downloadable ID is then

generated from the hashing of the Downloadable and the fetched components. *Id.* This reference is particularly telling because it addresses "the present invention" and not merely a preferred embodiment of the invention.

The claim, the specification, and the prosecution history, therefore, all require both the Downloadable and the fetched components to produce the Downloadable ID.[4]

VI. THE '822 PATENT

A. Construction of Claim Terms in the ''822 Patent

At the outset, it is important to recognize that the '822 Patent is based on a different specification than the '194 and '780 patents. The '822 patent also involves other named inventors.

1. Downloadable-Information

The term "downloadable-information" means "data downloaded from one computer to another" in the context of the '822 Patent. First, both parties agree that the term "downloadable-information" does not have an ordinary meaning. The claims also fail to provide any meaningful guidance to the meaning of the term. Consequently, it is appropriate to look to the specification.

a. The specification proves that downloadable-information is data downloaded from one computer to another.

The specification demonstrates that downloadable-information is any data downloaded from one computer to another. The specification provides a laundry list of information that can be considered downloadable-information, "including web pages, streaming media, transaction-facilitating information, program updates or other downloadable-information . . . [s]uch information can also include more traditionally

[4] Secure Computing has withdrawn its argument that the term "plugin" in the '780 Patent is indefinite as referenced in the Joint Claim Chart.

viewed 'Downloadables' or 'mobile code' (i.e. distributable components), as well as downloadable application programs or other further Downloadables." '822 Patent, JA53 at col.6 ll.1-12. The specification further states that "information received by server 301 (or firewall 302) can include non-executable information, executable information, or a combination of non-executable and one or more executable code portions." '822 Patent, JA55 at col.9 ll.14-17. All of these examples show that downloadable-information is anything that can be downloaded from one computer to another.

b. Finjan's Construction Contradicts the Intrinsic Evidence

Finjan proposes that the term "downloadable-information" means "a program or document that can contain mobile code." Much like in Finjan's definition of Downloadable in the '194 Patent, Finjan is again attempting to make the term "mobile code" synonymous with Downloadables. This definition, however, is at odds with the claims and specification. First, the claims indicate that downloadable information is analyzed for the presence of "executable code" not "mobile code." *See, e.g.*, '822 Patent, JA61 claim 1. Second, the specification, as cited above, shows that mobile code is merely a subset of information that is considered downloadable-information. '822 Patent, JA53 at col.6 ll.1-12 ("Such information can also include more traditionally viewed 'Downloadables' or 'mobile code' (i.e. distributable components), as well as downloadable application programs or other further Downloadables."). This discussion in the '822 Patent specification not only shows that Finjan's definition of downloadable-information is incorrect, but it also proves that "mobile code" is not synonymous with the term "Downloadable" as Finjan asserts in its construction of the term "Downloadable" in the '194 Patent.

2. Evaluating the detection indicators

The phrase "evaluating the detection indicators" means "evaluating two or more detection indicators to determine whether executable code is detected." This construction is based on the claim language itself and the description in the specification. For reasons unknown to Secure Computing, Finjan has refused to accept this construction.

Secure Computing's construction is straightforward based on the claim language itself. "Detection indicators" is plural, so there must be two or more of them that are evaluated.

3. Information-destination

The term "information-destination" means "a device or process that is capable of receiving and initiating or otherwise hosting a mobile code execution." Again, both sides agree that the term "information-destination" has no ordinary meaning. Again, the claims themselves do not assist us, so we must look to the specification.

The specification clearly spells out what is considered an information destination. The specification states that "[a] suitable information-destination or 'user device' can further include one or more devices or processes (such as email, browser or other clients) that are capable of receiving and initiating or otherwise hosting a mobile code execution." '822 Patent, JA 54 at col.7 ll.60-64.

Finjan's definition improperly limits the term "information-destination" to mean "client." Such a construction is both overinclusive and underinclusive. First, the term "client" may be underinclusive. If the term "client" is taken out of context of the '822 patent, an individual may mistakenly believe that a client could only be a device as opposed to a process. The specification expressly states, however, that an information-destination may be a process such as a browser. *See* '822 Patent, JA54 at col.7 ll.60-63

("[a] suitable information-destination or "user device" can further include one or more devices or processes (such as email, browser or other clients")) (emphasis added). Second, the term "client" is overinclusive, because it may include devices or processes that are incapable of receiving and initiating mobile code execution.

While Finjan is correct that an information-destination may include certain clients, that definition does not define the term in any meaningful way. Moreover, such a construction ignores the definition that the applicant provided to the public in the specification.

4. Information-recommunicator

An "information-recommunicator" is an "information-supplier or intermediary for servicing one or more further interconnected devices or processes or interconnected levels of devices or processes." This is another term that was created by the applicant, which has no ordinary meaning. Consequently, it is appropriate to focus on the specification for guidance.

The specification states that "[o]ne or more devices can also be configurable to operate as a network server, firewall, smart router, a resource server servicing deliverable third-party/manufacturer postings, a user device operating as a firewall/server, or other information-suppliers or intermediaries (i.e. as a "re-communicator" or "server") for servicing one or more further interconnected devices or processes or interconnected levels of devices or processes." '822 Patent, JA54 at col.7 ll.49-56. This is an explicit list of things that can be considered a "re-communicator."

Finjan proposes another oversimplified definition that is both over and underinclusive. The term "server" is not accurately descriptive of the definition that the applicants included in the specification. While it is true that a "server" may also be an

information-recommunicator, the two terms are not synonymous. The specification itself refers to a "'re-communicator' or 'server.'" Separating the terms by the word "or" suggests that the terms mean different things, even if there is some overlap.

In fact, if Finjan's goal is to define the limitations of information destination and information-recommunicator as synonymous with traditional client-server network configurations, the specification directly rejects such an approach. The specification states: "For clarity [sic] sake, a simple client-server configuration will be presumed unless otherwise indicated. It will be appreciated, however, that other configurations of interconnected elements might also be utilized (e.g. peer-peer, routers, proxy servers, networks, converters, gateways, services, network reconfiguring elements, etc.) in accordance with a particular application." '822 Patent, JA53 at col.6 l.63-col.7 l.2.

Based on the descriptions in the specification, Secure Computing's construction more appropriately and precisely defines the term "information-recommunicator."

5. Level of Downloadable-Information Characteristic and Executable Code Characteristic Correspondence

The phrase "level of downloadable-information characteristic and executable code characteristic correspondence" means "a value representing the degree of correspondence between the downloadable-information characteristic and the executable code characteristic." This definition is based on the claim language itself and the specification.

The disputed portion of this limitation is "level of . . . correspondence." The specification only refers to such a level of comparison once. '822 Patent, JA60 at col.19 ll.62-67. The specification uses the example of a weighted comparison between downloadable-information characteristics and executable code characteristics. *Id.* Based on this example and the common usage of the term "level," the patent is referring to some

value that represents a particular degree of correspondence between the downloadable-information characteristic and the executable code characteristic.

6. Several Terms in the '822 Patent are Indefinite under 35 U.S.C. § 112, ¶ 2 For Failure to Recite Sufficient Structure

Several of the claims in Finjan's patents are drafted in "means-plus-function" format but the terms are indefinite because the applicants did not recite sufficient structure for the corresponding function within the specification.

Section 112, paragraph 6 of the Patent Act provides that:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

35 U.S.C. § 112, ¶ 6. Thus, under paragraph 6, an applicant need not recite the structure in the claim itself so long as the specification recites sufficient structure for the performance of the function. Once the Court determines that a claim is written in "means-plus-function" language, the Court must make a two-step inquiry: "(1) the court must first identify the function of the limitation; and (2) the court must then look to the specification and identify the corresponding structure for that function." *Biomedino, LLC v. Waters Techs. Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007). As the Federal Circuit stated, "[i]f there is no structure in the specification corresponding to the means-plus-function limitation in the claims, the claim will be found invalid as indefinite." *Id.*

The first inquiry is whether certain terms in the claim are written in such a manner as to invoke the rules of "means-plus-function" language as provided by 35 U.S.C. § 112 ¶ 6. If a claim term uses the term "means" within the limitation, there is a presumption that the claim is governed by 35 U.S.C. § 112, ¶ 6. *Biomedino*, 490 F.3d at 949. On the

other hand, there is a rebuttable presumption that a claim is not governed by 35 U.S.C. § 112 ¶ 6 if the limitation does not recite the word "means." *Mas-Hamilton Group v. LaGard, Inc.*, 156 F.3d 1206, 1213 (Fed. Cir. 1998). As the Federal Circuit has noted, however, "such a presumption is helpful in beginning the claim construction analysis, [but] it is not the end of the inquiry." *Id.* The presumption can be overcome "even though the catch phrase is not used, [if] the limitation's language does not provide any structure, and [t]he limitation is drafted as a function to be performed rather than definite structure or materials." *Id.*

The following terms in the '822 patent have no customary or ordinary meaning to one of skill in the art. Even Finjan's own Chief Technology Officer, with years of computer security experience, admitted that the following terms do not have an ordinary meaning: packaging engine, content inspection engine, linking engine, transfer engine, and inspection controller. *See* Ben-Itzhak Depo., JA2148-52 at 101:17-105:6. The terms are purely functional limitations that do not recite necessary structure and consequently invoke the "means-plus-function" rules of 35 U.S.C. § 112 ¶ 6. The first term uses the term "means," so there is a presumption that it is a "means-plus-function" limitation.

Mobile Code Means -- The phrase "mobile code means" recites the term "means" consequently there is a presumption that it is a "means-plus-function" limitation. '822 Patent, claim 28. The claim recites several functions performed by the "mobile code means":

> mobile code means communicatively coupled to the receiving means for causing mobile protection code to be executed by a mobile code executor at a downloadable-information destination such that one or more operations of the executable code at the destination, if attempted, will be processed by the mobile protection code,

> wherein the causing is accomplished by forming a sandboxed package including the mobile protection code and the downloadable-information, and causing the sandboxed package to be delivered to the downloadable-information destination.

'822 Patent, JA62 claim 28 (emphasis added). In simplified terms, the mobile code means must cause code to be executed by forming a sandboxed package. No structure exists in the specification for performing this function. Consequently, the term is indefinite.

The remaining terms do not use the specific language of "means" in the limitation, however, the limitations are written in purely functional terms and lack structure in the specification. Consequently, the following terms still fall under 35 U.S.C. § 112, ¶ 6.

Content inspection engine – The claims use the phrase "content inspection engine" in only functional terms. A content inspection engine is used, according to the claims, "for determining whether the downloadable-information includes executable code." See '822 Patent, JA61 claim 9. The specification does not define or identify any structure for implementing an engine. In fact, there is no recitation of whether a content inspection engine is even mechanical, electrical, or software.

Packaging engine – This is another limitation defined in functional terms. According to Claim 9, a packaging engine is for "causing mobile protection code ("MPC") to be communicated to at least one information-destination of the downloadable-information." '822 Patent, JA 61 claim 9. The specification again fails to cite any structure for performing this function.

Linking Engine – Claim 12 defines linking engine in purely functional terms. The claim indicates that the linking engine is "for forming a sandbox package including

the MPC and the downloadable-information." '822 Patent, JA61 claim 12. The specification does not recite structure for this function.

Transfer Engine – Claim 12 describes a transfer engine functionally as something used "for causing the sandbox package to be communicated to the at least one information-destination." '822 Patent, JA61 claim 12. No corresponding structure is recited in the specification.

Inspection Controller – The patent only refers to an inspection controller once. '822 Patent, JA61 claim 9. In claim 9 an inspection controller is again described in functional terms, that is "for determining whether the indicators indicate that the downloadable-information includes executable code." *Id.* Again, no structure is recited in the specification for performing this function.

MPC generator – This term is used in Claim 12 and is described in functional terms. '822 Patent, JA61 claim 12. The term is merely defined as something used "for providing the MPC." *Id.* It is unclear what this even means functionally. Regardless, there is no recitation of structure in the specification to perform this function.

Policy generator – This limitation is included in Claim 13. '822 Patent, JA61 claim 13. Again, it is defined in functional terms only. The policy generator is described as something used "for providing protection policies according to which the MPC is operable." *Id.* No structure is recited in the specification.

All of the preceding claims in this section are governed by 35 U.S.C. § 112, ¶ 6 and fail to recite necessary structure. Consequently, this Court should construe these terms as indefinite under 35 U.S.C. § 112, ¶ 2.

Moreover, two phrases, "information monitor" and "destination-characteristics" have no ordinary meaning as admitted by Finjan's own CTO. *See* Ben-Itzhak depo. 8/10/07 at 103:14-104:18. The specification also lacks any definition for these terms. Consequently, these terms are also indefinite.

CONCLUSION

For the foregoing reasons Secure Computing respectfully requests that the Court reject Finjan's attempt to limit Secure Computing's claims to the minutia of the preferred embodiments while providing virtually no concrete limits on its own patents.

Kelly E. Farnan
Fredrick L. Cottrell, III (#2555)
cottrell@rlf.com
Kelly E. Farnan (#4395)
farnan@rlf.com
Richards, Layton & Finger
One Rodney Square
P.O. Box 551
Wilmington, DE 19899
(302) 651-7700
Attorneys For Defendants

OF COUNSEL:

Ronald J. Schutz
Jake M. Holdreith
Christopher A. Seidl
Trevor J. Foster
Robins, Kaplan, Miller & Ciresi L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500

Dated: September 7, 2007

UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on September 7, 2007, I electronically filed the foregoing with the Clerk of Court using CM/ECF and caused the same to be served on the defendant at the addresses and in the manner indicated below:

VIA ELECTRONIC MAIL & HAND DELIVERY

Philip A. Rovner
Potter Anderson & Corroon LLP
1313 N. Market Street,
Hercules Plaza, 6th Floor
Wilmington, DE 19899-0951

I further certify that on September 7, 2007, the foregoing document was sent to the following non-registered participants in the manner indicated:

VIA ELECTRONIC MAIL & FEDERAL EXPRESS

Paul J. Andre
Radhika Tandon
Perkins Coie LLP
101 Jefferson Drive
Menlo Park, CA 94025-1114

Kelly E. Farnan (#4395)